

Optimal für Unvorhergesehenes gerüstet

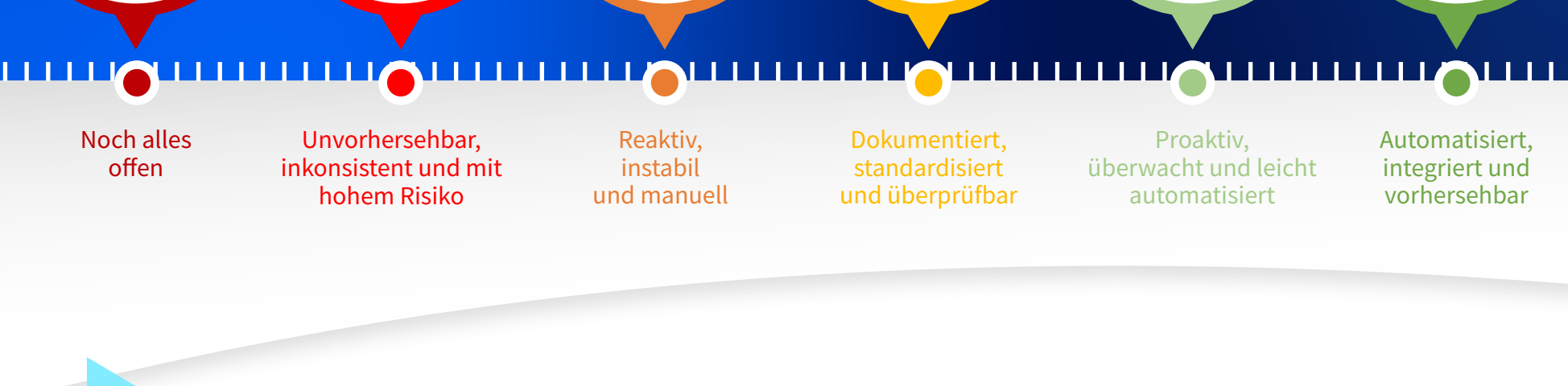
Was Sie über Datenschutz und Backup unbedingt wissen müssen

Den Datenschutz meistern



Die Reifegrade

Der Prozess erfordert Reflexion, Zeit und Investitionen. Mit geeigneten und zielgerichteten Maßnahmen können Sie in Ihrem Tempo voranschreiten.



Downtime & Loss

Mit dem exponentiellen Wachstum des Datenvolumens und immer mehr Unternehmen, die sich als „data driven“ bezeichnen, sind die Risiken höher denn je.



Ein immer komplexeres Thema

Datengestützte Organisationen „data driven“ haben mit zunehmender Komplexität in den Bereichen Datenschutz und Disaster Recovery zu kämpfen.



Die harte Realität

Die auf Daten abzielenden Bedrohungen werden immer zahlreicher und spitzen sich zu. Und die Folgen dieser Bedrohungen werden tendenziell immer gravierender.

Im Jahr 2021



Woher kommen die Bedrohungen?

Sie können interner oder externer Natur sein: Quellen gibt es viele.



3-2-1-Backup-Strategie



Die umfassende Strategie für Datenschutz:

- 1. Alle Risiken bewerten**
Identifizieren Sie alle Bedrohungen, denen Ihr Unternehmen ausgesetzt sein könnte, sowie die sensibelsten/kritischsten Daten.
- 2. Zugehörige Ziele definieren**
Was muss für Business Continuity implementiert werden?
Wie lauten die Zielvorgaben für die Wiederherstellungszeit (Recovery Time Objective, **RTO**) und den maximalen Datenverlust (Recovery Point Objective, **RPO**) für Ihre Systeme und Anwendungen bei einem Ausfall, wobei zwischen nicht kritisch, wesentlich und kritisch unterschieden wird?

NEUSTART DER ANWENDUNG

Recovery Time Objective

RPO

Recovery Point Objective

ZULETZT NUTZBARE DATEN
- 3. Eine maßgeschneiderte Strategie erarbeiten**
Wählen Sie eine geeignete Disaster-Recovery-Strategie (Cold, Warm oder Hot) oder entscheiden Sie sich für einen cloudgestützten Disaster Recovery Plan (DRP), um die Vorteile der Cloud zu nutzen.
- 4. Testen und wiederholen**
Überprüfen Sie regelmäßig, ob Ihre Strategie immer noch Ihren Anforderungen entspricht und ob sie auch effektiv ist.
- 5. Verfahren dokumentieren**
Machen Sie klare und präzise Angaben zu allen Aspekten Ihres Disaster Recovery Plan, einschließlich der Reaktionsverfahren, der Kommunikation und der Systemwiederherstellung.
- 6. Mitarbeiter:innen schulen und informieren**
enken Sie daran, Ihre Kolleg:innen über Best Practices für die IT-Sicherheit zu informieren.
- 7. Überwachen, pflegen und aktualisieren**
Rüsten Sie sich für das Aufspüren verdächtiger Aktivitäten und eine schnelle und effektive Reaktion. Überprüfen und aktualisieren Sie Ihren DRP regelmäßig, um sicherzustellen, dass er relevant und bei Angriffen und aufkommenden Problemen geeignet ist.

#MoveToCloud



Vor der Migration

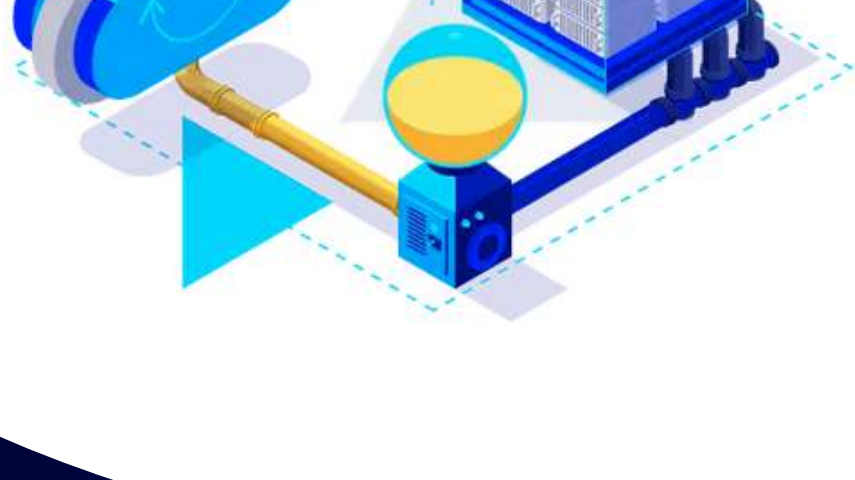
- **Überprüfen** Sie die Backup-Dienste, die in die verwendeten Lösungen integriert sind.
- **Informieren** Sie sich über aktuelle und zukünftige Standard-Speicherlösungen, die sicher und auf Ihre Anforderungen zugeschnitten sind (Compliance, Leistung, Preis usw.).
- **Denken** Sie auch an die Replikation Ihrer Daten (Kopien und Speicherung an mehreren Orten), um deren Verfügbarkeit und Zugänglichkeit zu verbessern.

Anbieter

Bevor Sie sich entscheiden, empfehlen wir Ihnen, die angebotenen Leistungen ausführlich darzulegen: Compliance, Souveränität, SLA, Reversibilität usw.

OVHcloud

Mehr als 20 Jahre Erfahrung



- **Hochresiliente,** zertifizierte und sichere Infrastrukturen, die integrierte und interoperable Dienste hosten
- **Planbare Rechnungen** ohne versteckte Kosten, damit Sie Ihre Investitionen genau kontrollieren können
- **Ein spezialisiertes Ökosystem,** bestehend aus den wichtigsten Akteuren im Datenschutz (NetApp, Nutanix, Veeam, VMware, Zerto) und einem Netzwerk mit mehr als 1.000 Partnern

Quellen:

¹ Laut Moore's Law, einer empirischen Beobachtung des Mitgründers von Intel, die durch zahlreiche Forschungsberichte und Studien bestätigt wird, darunter Veröffentlichungen von IDC und der EMC Corporation

² Laut einer Schätzung aus dem im Mai 2022 veröffentlichten Whitepaper *The State of Ransomware and Disaster Preparedness* von IDC

³ Laut einer Schätzung aus der IBM-Studie *Cost of a Data Breach Report* aus dem Jahr 2020

⁴ Laut dem Jahresbericht *The Cost of a Data Breach* des Ponemon Institute aus dem Jahr 2021

⁵ Laut Jahresbericht *2021 SonicWall Cyber Threat*

Infografik erstellt im Juni 2023